SCADA Field Device Protection Profile Project

Milestone 2: TOE Security Environment

Introduction

The Process Control Security Requirements Forum (PCSRF) has a project to develop and complete a SCADA Field Device Protection Profile by April 30, 2006. The Protection Profile will list the security requirements for field devices such as PLC's, PAC's, RTU's and IED's.

The Protection Profile is an opportunity for asset owners, vendors, industry organizations, government organizations and other interested parties to provide a clear and comprehensive set of security requirements for the next generation of SCADA field devices. Vendors will then be able to develop field devices that meet the Protection Profile requirements and have those devices independently tested and certified by an internationally recognized third party.

PCSRF has chosen to use the Common Criteria methodology to specify functional and assurance requirements. The Common Criteria has a precise language and methodology that enables for clear specifications and objective testing. To achieve this, the Common Criteria sacrifices readability and is not the appropriate document for a general reader to learn guidelines or best practices. It may not be easy for even a subject matter expert in SCADA Field Devices to understand some of the later sections of the Protection Profile text.

To encourage participation each milestone deliverable in this project will have a section with the draft Protection Profile text and a section explaining the Protection Profile text. We need your comments on either the Protection Profile text or the explanatory text. If you can identify an issue in the explanatory text, we can convert it into the proper Common Criteria format.

There are helpful books available, such as Debra Herrmann's *Using the Common Criteria for IT Security Evaluations*, if you want to understand the specific Common Criteria language. As Ms. Herrman defines it, the Common Criteria "provide a complete methodology, notation, and syntax for specifying requirements, designing a security architecture, and verifying the security integrity of an 'as built' product, system or network."

Milestone 2 covers the TOE Security Environment for a Protection Profile. The assumptions about the environment, threats against the TOE, and organizational policies are enumerated and defined in this section. Later sections will include specific security objectives and functional requirements that mitigate these threats.

PLEASE SUBMIT COMMENTS FOR MILESTONE 2 BY DECEMBER 7, 2005

SUBMIT COMMENTS TO: peterson@digitalbond.com

11/30/2005

- - - Begin Protection Profile Text - - -

TOE Security Environment

Assumptions

The specific conditions below are assumed to exist in a TOE environment.

A.AuthorizedUsers Authorized users and administrators will not attack the TOE if they are acting within the authorization limits enforced by the TOE's access control mechanisms.

A.ModerateExposure The threat of malicious attacks aimed at discovering and exploiting vulnerabilities is considered moderate.

A.PhysicalAccess The TOE will be placed in a secure physical location which will prevent unauthorized physical access and modification.

A.PhysicalEnvironment The TOE will receive adequate power and be located in an environment that meets the Security Target's environmental specifications.

Threats

The threats listed below are addressed by Protection Profile compliant TOE's. The threat agents are either unauthorized persons, unauthorized IT devices, or disgruntled insiders exceeding their authorized use of the TOE. All threat agents are jointly described as an 'attacker' in the threats below.

T.CredentialCracking An attacker may repeatedly try to guess authentication credentials in order to gain unauthorized access to the TOE.

T.DataAlteration An attacker may intercept and modify communication sent to or from the TOE in an attempt to force an unauthorized action or affect the integrity of the TOE.

T.DataFlooding An attacker may send a large volume of data to the TOE to restrict the availability of the TOE. This threat may also be used to attempt to cause the TOE to improperly process data due to limited computing resources.

T.EscalationOfPrivilege An attacker who has already gained authorized access to the TOE may attempt to increase its authorization rights by attacking the access control configuration.

T.Hijacking An attacker may attempt to hijack an existing authorized session to gain the privileges of the user or device in the existing session.

T.MalformedData An attacker may attempt to compromise the availability or integrity of a TOE by sending malformed data to the TOE.

Malformed data is data that does not comply with the expected protocol. It could be values outside of the permitted range, random modifications of the protocol, or data generated using protocol fuzzing tools.

T.Reconnaissance An attacker may attempt to gather information about the TOE, the TOE configuration, or information in the TOE for use in a future attack or to compromise the confidentiality of the TOE information.

T.Replay An attacker may record valid communication sent to the TOE and replay all or a portion of the communication to attempt to fool the TOE into performing an unauthorized action or response.

T.Spoofing An attacker may represent itself as a valid user or device by spoofing the IP address or some other identifying parameter to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

T.StoredDataAttack An attacker may delete or modify information stored in the TOE to prevent proper operation or to destroy evidence of the attack.

T.SystemIntegrity An attacker may attempt to replace or destroy application code, configuration parameters or system data in the TOE to compromise the availability or integrity of the TOE.

T.UnauthenticatedAccess An attacker may bypass the authentication mechanism to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

T.UnauthorizedAction An attacker that has been authenticated may attempt to perform an unauthorized action by circumventing security in the access control mechanisms.

Organizational Security Policies

Protection Profile compliant TOE’s must address the organizational security policies described below.

P.ApprovedCrypto The TOE shall use FIPS-approved security functions and NIST FIPS validated implementations for all cryptographic functions including key management, hashing, encryption, digital signatures, and random number generation.

P.Communication The organization shall insure communication to and from the TOE is available.

- - - End Draft Protection Profile Text - - -

Open Issues

There were a small number of threats and organizational security policies that were considered but were not included. Some of these were tough decisions, and the group should provide feedback on the following three possible additions to this section.

Eavesdropping / Confidentiality

The TOE boundary is the physical enclosure and interfaces of a PLC, RTU or IED. Therefore, the threats to the communication channels are outside of the TOE. Nevertheless, there are threats included in this section that address the integrity and availability of the communication that arrives at the TOE boundary, such as T.MalformedData, T.Replay, T.Spoofing and T.DataFlooding. The TOE Security Environment does not include any assumptions, threats or policies addressing a breach in confidentiality of communication to or from the TOE.

In most cases, confidentiality is significantly less important than availability or integrity for a field device. It may be overkill to require confidentiality protection to address an eavesdropping or sniffing threat, and the Protection Profile would not preclude a vendor adding security functional requirements to cover encryption. This requirement also could be handled in a future composite Protection Profile that covered various components of a SCADA system, including field devices, and the communication between these components.

Even with the above reasons not to include eavesdropping as a threat, this was a difficult call that requires some additional input. Below is a draft threat and organizational security policy for the group's consideration that could be added to the Protection Profile.

T.Eavesdropping — An attacker may eavesdrop or sniff communication to or from the TOE thereby compromising the confidentiality of the information outside of the TOE.

Or

P.SecureChannel — The organization shall provide protected communication channels for authorized request and response messages sent outside the TOE.

Administrative Access

The draft section identifies a number of threats that are universal to any user role or any device. For example, all communication with the TOE is susceptible to an attacker circumventing authentication or access control mechanisms. All communication with the TOE could be altered, spoofed or hijacked. These are not unique threats to administrative access, so the draft does not have any specific assumptions, threats, or organizational security policies for administrative access.

We did draft and consider adding the organizational security policy listed below.

P.AdminAccess — Administrators shall be able to administer the TOE both locally and remotely through protected communication channels.

Vulnerability Analysis Testing

Independent vulnerability testing of equipment or systems often identifies vulnerabilities that developers may miss because they are too close to the product or have a test process to closely correlated with the design. Some Protection Profiles, such as the U.S. Government Firewall Protection Profile for Medium Robustness, have an organizational security policy that requires a vulnerability assessment. The Firewall Protection Profile example is below:

P.VulnerabilityAnalysisTest The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

This organizational security policy was ultimately not included in the draft because vulnerability testing of field devices is a relatively new field. There are tools and examples from BCIT, Langner Communications and a few others, but there is not an industry consensus yet as to what an "appropriate independent vulnerability analysis and penetration test" would be. There may however be a consensus on this issue by the time the Security Targets are undergoing certification testing.

Explanatory Text

This section of the Common Criteria defines the security environment for the TOE and is the first step in a three part rationalization, or mapping, which is required and will take place in the Protection Profile. The steps are:

1. Define the security environment by enumerating and defining the Assumptions, Threats, and Organizational Security Policies. This is done in this draft.
2. Define the TOE Security Objectives and the TOE Environment Security Objectives. Map the Objectives to the Assumptions, Threats and Organizational Security Policies they address. Each Assumption, Threat and Organizational Security Policy must be addressed by one or more Objectives. The Objectives will be developed in Milestone 3 in this project.
3. Define the Security Functional Requirements. Map the Security Functional Requirements to the Objectives they address. Each TOE Security Objective must be addressed by a Security Functional Requirement. The TOE Environmental Security Objectives are addressed by the environment rather than the TOE and are not necessarily addressed by Security Functional Requirements. The Security Functional Requirements will be addressed in Milestone 4 in this project.

This rationalization insures that each threat is addressed. Conversely, it prevents objectives and security functional requirements being added that do not address any enumerated threat.

The reasons for including the assumptions, threats and organizational security policies are not included in the Protection Profile. For the sake of peer review and understanding we included some reasons and explanatory text below.

Assumptions are givens about the TOE or the TOE environment. Assumptions cannot be used to mitigate threats.

A.AuthorizedUsers

Authorized users and administrators will not attack the TOE if they are acting within the authorization limits enforced by the TOE's access control mechanisms.

Comment: This assumption is to make clear the Protection Profile will not prevent an authorized user from taking an authorized action, even if the action is an unintentional mistake or a malicious act. For example, if an administrator is authorized to clear the audit logs, the Protection Profile will not prevent the administrator from clearing the logs.

A.ModerateExposure

The threat of malicious attacks aimed at discovering and exploiting vulnerabilities is considered moderate.

Comment: Protection Profiles typically make a general assumption of the skill level and motivation of the attacker. A moderate level was selected because the TOE is a field device rather than a critical SCADA server, but it is a device that will be used in many critical infrastructure systems that may be targets for cyberterrorists and other highly skilled and motivated attacker. We considered raising this to A.HighExposure.

A.PhysicalAccess

The TOE will be placed in a secure physical location which will prevent unauthorized physical access and modification.

Comment: The Protection Profile assumes the attacks will be limited to cyber attacks because the field device will be in a physically secure location. There are no threats related to physical security. It would be possible to add these threats and include some level of tamper resistance or tamper evidence in the functional requirements.

A.PhysicalEnvironment

The TOE will receive adequate power and be located in an environment that meets the Security Target's environmental specifications.

Comment: The Protection Profile assumes the physical environment itself will not be used to attack the TOE. Power, temperature and humidity are available at the appropriate settings.

The enumerated threats will have the biggest impact on the Protection Profile and resulting future secure field devices and deserve a close review.

T.CredentialCracking

An attacker may repeatedly try to guess authentication credentials in order to gain unauthorized access to the TOE.

Comment: This is a straightforward password cracking or guessing threat. Once the credentials are recovered the attacker can gain access to the TOE.

T.DataAlteration

An attacker may intercept and modify communication sent to or from the TOE in an attempt to force an unauthorized action or affect the integrity of the TOE.

Comment: Altering the data sent to or from the TOE can impact security in a variety of ways. This is extremely important if there are limited security checks in the communication, such as only an address check or a simple checksum. An attacker could modify a read, write or diagnostic command sent to the TOE. Communication from the TOE could be modified to mislead the receiving system to the actual state of the PLC or underlying process.

T.DataFlooding

An attacker may send a large volume of data to the TOE to restrict the availability of the TOE. This threat may also be used to attempt to cause the TOE to improperly process data due to limited computing resources.

Comment: This is a brute force denial of service attack. It could be a small number of large requests, a large number of small requests, or any other combination of messages that prevents legitimate communication. The data flooding could overwhelm the communication bandwidth or the computing resources of the TOE.

T.EscalationOfPrivilege

An attacker who has already gained authorized access to the TOE may attempt to increase its authorization rights by attacking the access control configuration.

Comment: Escalation of Privilege is a common attack in IT where an authorized user tries to gain administrator or superuser privileges.

T.Hijacking

An attacker may attempt to hijack an existing authorized session to gain the privileges of the user or device in the existing session.

Comment: If security is limited to the initiation of a session, an attacker could wait until a session was in place and then hijack the session.

T.MalformedData

An attacker may attempt to compromise the availability or integrity of a TOE by sending malformed data to the TOE. Malformed data is data that does not comply with the expected protocol. It could be values outside of the permitted range, random modifications of the protocol, or data generated using protocol fuzzing tools.

Comment: Based on early testing by a number of industry research organizations, malformed data causes many field devices to crash. Many of the existing field devices were tested by the vendors for proper operation with proper data, but not proper operation with malformed data.

Some of this malformed data is sent in vulnerability scanning tools that are known to crash field devices. Additionally, attackers can fuzz, or slightly modify a protocol, and send it to a field device. The field device may crash or act in an unauthorized manner if the data varies from the expected protocol.

T.Reconnaissance

An attacker may attempt to gather information about the TOE, the TOE configuration, or information in the TOE for use in a future attack or to compromise the confidentiality of the TOE information.

Comment: Diagnostic reconnaissance commands could identify the vendor/product/version of the TOE which will help an attacker research vulnerabilities and craft future attacks. Reading individual points or scanning all the coils and registers can provide information about the TOE and process that may be used in a subsequent cyber or physical attack.

T.Replay

An attacker may record valid communication sent to the TOE and replay all or a portion of the communication to attempt to fool the TOE into performing an unauthorized action or response.

Comment: All or parts of requests to the TOE could be replayed. For example, a reboot command could be recorded and replayed repeatedly to create a denial of service attack. A valid request for a process shutdown could be recorded and replayed. The security fields in a message could be recorded and replayed in combination with a T.DataAlteration attack.

T.Spoofing

An attacker may represent itself as a valid user or device by spoofing the IP address or some other identifying parameter to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

Comment: This is similar to data alteration and hijacking, but in spoofing the attacker initiates the session. The attacker attempts to fool the TOE by impersonating an authorized user or device.

T.StoredDataAttack

An attacker may delete or modify information stored in the TOE to prevent proper operation or to destroy evidence of the attack.

Comment: The TOE will have field device information in points that are necessary for proper operation and in logs that document past operation. An attacker may want to disrupt operations, blind the control center or HMI to the process status, or cover his tracks by deleting this data. A more sophisticated attacker may modify the data to mislead the authorized users and fool them into taking the wrong action or no action, thereby delaying the correct response.

T.SystemIntegrity

An attacker may attempt to replace or destroy application code, configuration parameters or system data in the TOE to compromise the availability or integrity of the TOE.

Comment: This threat is similar to stored data attack, but this deals with the integrity of the system and application code rather than the process data or logs. This would be similar to the difference between the integrity of a database application and the database itself. Both are important, but they are different threats.

T.UnauthenticatedAccess

An attacker may bypass the authentication mechanism to attempt to compromise the integrity or availability of the TOE or the confidentiality of information in the TOE.

Comment: This threat presupposes that users and devices will be authenticated. There are attacks that try to fool an application that an authenticated session already exists.

T.UnauthorizedAction

An attacker that has been authenticated may attempt to perform an unauthorized action by circumventing security in the access control mechanisms.

Comment: Authenticated users can attempt to exceed their authorized rights. An operator can try to perform actions restricted to administrators. This threat will lead to access control objectives and requirements that will enforce authorization rights. It is related to the escalation of privilege threat, but unauthorized actions can take place in a weak system without gaining the required privilege.

Organizational security policies are typically addressed in later sections by security objectives for the TOE environment rather than security objectives for the TOE and security functional requirements.

P.ApprovedCrypto

The TOE shall use FIPS-approved security functions and NIST FIPS validated implementations for all cryptographic functions including key management, hashing, encryption, digital signatures, and random number generation.

Comment: Since this standard is developed under a NIST sponsored program and NIST is the organization that creates the standards for unclassified systems and communication, this policy seemed to be an obvious choice.

P.Communication

The organization shall insure communication to and from the TOE is available.

Comment: There will be no security functional requirements related to the availability of communication channels to and from the TOE because this is outside of the TOE's control. However this communication path is required for proper TOE operation. This could be an assumption or a policy.

Acronyms

DCS	Distributed Control System
IED	Intelligent Electronic Device
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller
PP	Protection Profile
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TOE	Target of Evaluation
TSF	TOE Security Functions

Next Milestone: Security Objectives

PLEASE SUBMIT COMMENTS FOR MILESTONE 2 BY DECEMBER 7, 2005

SUBMIT COMMENTS TO: peterson@digitalbond.com